



OFFICE OF AUDITOR OF STATE
STATE OF IOWA

State Capitol Building
Des Moines, Iowa 50319-0004

Telephone (515) 281-5834 Facsimile (515) 242-6134

David A. Vaudt, CPA
Auditor of State

NEWS RELEASE

FOR RELEASE _____ July 27, 2010

Contact: Andy Nielsen
515/281-5834

Auditor of State David A. Vaudt today released a report on the review of selected general and application controls over the State University of Iowa (University of Iowa) ePro System for the period June 15, 2009 through July 31, 2009.

Vaudt recommended the University of Iowa develop and implement procedures to improve information system password controls and segregation of duties.

A copy of the report is available for review at the University of Iowa, in the Office of Auditor of State and on the Auditor of State's web site at <http://auditor.iowa.gov/reports/1061-8010-BT01.pdf>

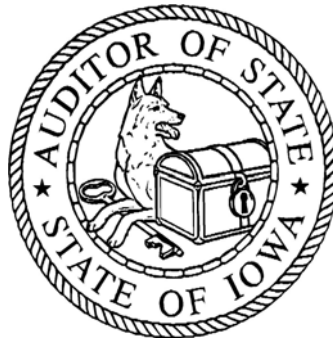
#

**REPORT OF RECOMMENDATIONS TO THE
STATE UNIVERSITY OF IOWA
ON THE REVIEW OF SELECTED GENERAL
AND APPLICATION CONTROLS OVER
THE UNIVERSITY'S EPRO SYSTEM**

JUNE 15, 2009 THROUGH JULY 31, 2009

Office of
**AUDITOR
OF STATE**

State Capitol Building • Des Moines, Iowa



David A. Vaudt, CPA
Auditor of State



OFFICE OF AUDITOR OF STATE
STATE OF IOWA

David A. Vaudt, CPA
Auditor of State

State Capitol Building
Des Moines, Iowa 50319-0004

Telephone (515) 281-5834 Facsimile (515) 242-6134

June 22, 2010

To the Members of the
Board of Regents, State of Iowa:

In conjunction with our audit of the financial statements of the State University of Iowa (University of Iowa) for the year ended June 30, 2009, we conducted an information technology review of selected general and application controls for the period June 15, 2009 through July 31, 2009. Our review focused on the general and application controls of the University's ePro System as they relate to our audit of the financial statements. The review was more limited than would be necessary to give an opinion on internal controls. Accordingly, we do not express an opinion on internal controls or ensure all deficiencies in internal controls are disclosed.

In conducting our review, we became aware of certain aspects concerning information technology controls for which we believe corrective action is necessary. As a result, we have developed recommendations which are reported on the following pages. We believe you should be aware of these recommendations which pertain to the University's general and application controls over the ePro system. These recommendations have been discussed with University personnel and their responses to these recommendations are included in this report. While we have expressed our conclusions on the University's responses, we did not audit the University's responses and, accordingly, we express no opinion on them.

This report, a public record by law, is intended solely for the information and use of the officials and employees of the University of Iowa, citizens of the State of Iowa and other parties to whom the University of Iowa may report. This report is not intended to be and should not be used by anyone other than these specified parties.

We would like to acknowledge the many courtesies and assistance extended to us by personnel of the University during the course of our review. Should you have questions concerning any of the above matters, we shall be pleased to discuss them with you at your convenience. Individuals who participated in our review of the ePro system are listed on page 6 and they are available to discuss these matters with you.

DAVID A. VAUDT, CPA
Auditor of State

WARREN G. JENKINS, CPA
Chief Deputy Auditor of State

cc: Honorable Chester J. Culver, Governor
Richard C. Oshlo, Jr., Director, Department of Management
Glen P. Dickinson, Director, Legislative Services Agency

Report of Recommendations to the University of Iowa

June 15, 2009 through July 31, 2009

ePro System Controls

A. Background

The ePro system at the State University of Iowa (University) is a web-based system consisting of the e-Voucher and PReq applications. The e-Voucher application allows departments to create payment vouchers for services and other non-purchase order payments. PReq allows departments to create requisitions used by Purchasing to create purchase orders. Under the ePro system, documents are routed for completion and for approvals following a predetermined path.

B. Scope and Methodology

In conjunction with our audit of the financial statements of the University, we reviewed selected aspects of the general and application controls in place over the University's ePro system for the period June 15, 2009 through July 31, 2009. Specifically, we reviewed the general controls: security program, access controls, configuration management controls, segregation of duties and service continuity and the application controls: input, processing and output controls. We interviewed staff of the University and we reviewed University policies and procedures. To assess the level of compliance with identified controls, we performed selected tests.

We planned and performed our review to adequately assess those University operations within the scope of our review. We developed an understanding of the University's internal control relevant to the operations included in the scope of our review. We believe our review provides a reasonable basis for our recommendations.

We used a risk-based approach when selecting activities to be reviewed. We focused our review efforts on those activities we identified through a preliminary survey as having the greatest probability for needing improvement. Consequently, by design, we use our finite review resources to identify where and how improvements can be made. Thus, we devote little effort to reviewing operations that may be relatively efficient or effective. As a result, we prepare our review reports on an "exception basis." This report, therefore, highlights those areas needing improvement and does not address activities that may be functioning properly.

C. Results of the Review

As a result of our review, we found certain controls can be strengthened to further ensure the reliability of financial information. Our recommendations, along with the University's responses, are detailed in the remainder of this report.

Report of Recommendations to the University of Iowa

June 15, 2009 through July 31, 2009

General Controls

- (1) **Password Controls**–User ID's and passwords are used to identify and authenticate users in controlling access to system resources. Passwords, however, are not conclusive identifiers of specific individuals since they may be compromised. Typical controls for protecting the confidentiality of passwords include requirements they be changed every 60 to 90 days, not allowed to be reused and locked after a limited number of consecutive unsuccessful attempts. Password controls for the ePro system could be strengthened.

Recommendation – The University should implement security features to strengthen password controls for the ePro system.

Response–A revised enterprise password policy draft is currently under a campus review period. Our protocol for policy development includes a period to allow for feedback from community members to ensure IT policy meet our needs and are consistent with the University's mission and goals. Technology changes planned for implementation will soon allow for use of multiple operational policies. The revised password policy leverages this change, by making a distinction between users with privilege access to resources and data, and will allow us to more appropriately manage risk with stronger policy controls for those individuals.

Conclusion–Response accepted.

- (2) **Workflow Segregation of Duties**–University department and organization workflow administrators have been given the responsibility for setting up workflow approvals for their departments or organizations to control the approvals required for financial transactions. There does not appear to be any formal guidance to ensure the control environment stresses proper segregation of duties.

Recommendation – The University should provide guidance for departmental and organizational workflow administrators to ensure an environment stressing segregation of duties and internal control responsibilities is maintained.

Response–Guidance on segregation of duties and internal control responsibilities for departmental and organizational workflow administrators is provided through various departmental training classes: Procure to Pay, Business Process Series, Sub Certification Training and E-Voucher training. This guidance will be documented in a formal procedures document and made available to workflow administrators.

Conclusion–Response accepted.

Application Controls

No recommendations were noted in our review of application controls for the University's ePro system.

Report of Recommendations to the University of Iowa

June 15, 2009 through July 31, 2009

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Gwen D. Fangman, CPA, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated in this review include:

Daniel L. Grady, Senior Auditor
Shawn R. Elsbury, Senior Auditor
Aaron Wagner, CPA, Staff Auditor
Kristin M. Ockenfels, Assistant Auditor